

CLAIMS

What is claimed is:

1. A portable device comprising:
a microprocessor;
a non-volatile memory coupled to the microprocessor; and
a biometrics-based authentication module coupled to and controlled by the microprocessor, wherein access to the non-volatile memory is granted to a user provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the non-volatile memory is denied to the user otherwise.
2. The portable device as recited in Claim 1 wherein the biometrics-based authentication module is a fingerprint authentication module.
3. The portable device as recited in Claim 1 further comprising a universal serial bus (USB) connector for coupling with another USB-compliant device.
4. The portable device as recited in Claim 1 wherein the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the portable device.
5. The portable device as recited in Claim 1 wherein the non-volatile memory comprises flash memory.
6. The portable device as recited in Claim 1 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.
7. A portable device comprising:
a bus;
a microprocessor coupled to the bus;
a non-volatile memory coupled to the bus; and
a biometrics-based authentication module coupled to the bus, wherein under the control of the microprocessor the biometrics-based authentication module is configured to

(1) capture a first biometrics marker; (2) store the first biometrics marker in the non-volatile memory; (3) capture a second biometrics marker; and (4) determine whether the second biometrics marker can be authenticated against the first biometrics marker.

8. The portable device as recited in Claim 7 wherein the biometrics-based authentication module is a fingerprint authentication module.

9. The portable device as recited in Claim 7 further comprising a universal serial bus (USB) device controller coupled to the bus and a USB connector coupled to the bus, such that the portable device is capable of communicating with a host platform via the USB connector.

10. The portable device as recited in Claim 7 wherein the biometrics-based authentication module is structurally integrated with the portable device in a unitary construction and comprises a biometrics sensor being disposed on one surface of the portable device.

11. The portable device as recited in Claim 7 wherein the non-volatile memory comprises flash memory.

12. The portable device as recited in Claim 7 wherein the biometrics-based authentication module is further configured to encrypt the first biometrics marker before storing the first biometrics marker in the non-volatile memory.

13. The portable device as recited in Claim 7 wherein the microprocessor is configured to direct the biometrics-based authentication module to capture and store the first biometrics marker provided that no biometrics marker has been stored in the non-volatile memory.

14. The portable device as recited in Claim 7 wherein the microprocessor is configured to enable access to the non-volatile memory upon a determination of authentication success by the biometrics-based authentication module.

15. The portable device as recited in Claim 7 wherein the microprocessor is configured to disable access to the non-volatile memory upon a determination of authentication failure by the biometrics-based authentication module.

16. The portable device as recited in Claim 7 wherein the microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module.

17. A biometrics-based authentication method implemented using a portable device, the method comprising the steps of:

- (a) obtaining a first biometrics marker from a user with a biometrics sensor installed on the portable device;
- (b) retrieving a registered biometrics marker from a memory of the portable device, the registered biometrics marker having been stored therein during a registration process;
- (c) comparing the first biometrics marker against the registered biometrics marker; and
- (d) signaling an authentication success provided that a match is identified in said step (c).

18. The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is a fingerprint.

19. The biometrics-based authentication method as recited in Claim 17 wherein the registered biometrics marker is stored in an encrypted format.

20. The biometrics-based authentication method as recited in Claim 17 wherein said step (d) comprises granting the user access to the non-volatile memory.

21. The biometrics-based authentication method as recited in Claim 17 further comprising the step of denying the user access to the non-volatile memory provided that a match is not identified in said step (c).

22. The biometrics-based authentication method as recited in Claim 17 further comprising the step of providing the user with a bypass authentication procedure provided that a match is not identified in said step (c).

09898365-070304